(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
13. Januar 2005 (13.01.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/003933 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, 17/30

(21) Internationales Aktenzeichen: PCT/DE2004/001252

(22) Internationales Anmeldedatum:
17. Juni 2004 (17.06.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 29 779.0 1. Juli 2003 (01.07.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KÖPPEN, Siegried** [DE/DE]; Chausseestr. 60, 15711 Königs-Wusterhausen (DE). **LÖWE, Stefan** [DE/DE]; Kaiserin-Auguste-Allee 95, 10589 Berlin (DE).

(74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente)R8-10, Am Kavalleriesand 3, 64295 Darmstadt (DE).

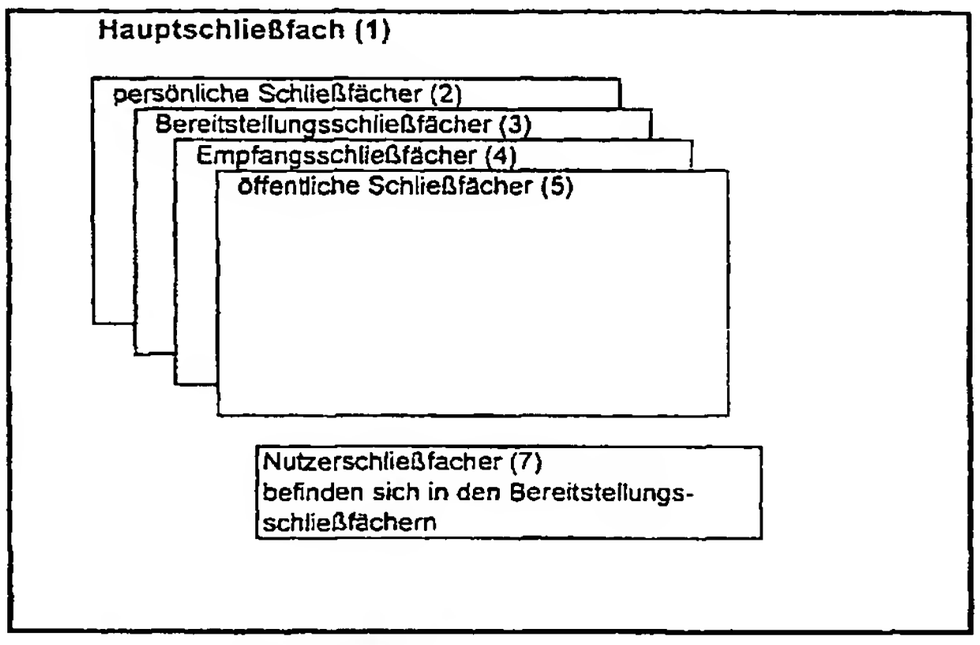
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR USE IN A NETWORK BASED SAFETY DATA STORAGE SYSTEM

(54) Bezeichnung: VERFAHREN FÜR EIN NETZBASIERTES DATENSPEICHERSYSTEM MIT HOHER SICHERHEIT



1 MAIN LOCKER
2 PERSONAL LOCKERS
3 PROVISIONING LOCKERS
4 RECEIVING LOCKERS
5 PUBLIC LOCKERS
7 USER LOCKERS ARE LOCATED IN THE PROVISIONING LOCKERS

(57) **Abstract:** The invention relates to a method for use in a data storage system which applies high safety requirements for the storage of data on a server in a telecommunications network and for the retrieval of the files by the local computers linked with the server via the network. The applicant is provided with a user certificate and public and secret keys, preferably on a chip card. Once the server is dialed up via the internet, a client program is forwarded to the user which controls authentication of the user and the transmission of additional safety-relevant features of proof such as biometrical systems, geographical positioning, time-dependent data, network and computer data etc. to the server. The storage system on the server is provided with a locker-type characteristic by establishing folders comprising a specific file for the safety requirements related thereto. The lockers are distinguished by their specific function and are only displayed to the user when the safety requirements are met. This locker system thus also has virtual character.

[Fortsetzung auf der nächsten Seite]

WO 2005/003933 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren für ein Datenspeichersystem, bei dem für die Speicherung der Daten auf einem Server in einem Telekommunikationsnetz und den Abruf der Dateien durch die über das Netz mit dem Server verbundenen lokalen Rechner hohe Sicherheitsanforderungen vorgegeben werden. Nutzerzertifikat sowie öffentlicher und geheimer Schlüssel werden dem Antragsteller vorzugsweise auf einer Chipkarte bereitgestellt. Nach Anwahl des Servers über das Internet wird dem Nutzer ein Clientprogramm zugesandt, das die Authentifizierung des Nutzers sowie die Übertragung weiterer sicherheitsrelevanter Nachweise wie biometrische Systeme, geografische Positionsbestimmung, Zeitabhängigkeiten, Netz- und Rechnerdaten u.a. zum Server steuert. Das Speichersystem auf dem Server erhält Schließfachcharakter, indem jeder Ordner mit einer speziellen Datei für die auf ihn bezogenen Sicherheitsanforderungen eingerichtet wird. Die Schließfächer werden nach Funktionen unterschieden und kommen für die Nutzer nur zur Anzeige, wenn die Sicherheitsbedingungen erfüllt sind. Damit hat Schließfachsystem einen virtuellen Charakter.